Claims

1. Method for control of usage of content, the method comprising the steps of
   - obtaining the content at a user device (D1),
   - defining at least one usage right at the user device (D1), the at least one defined usage right specifying one or more usage restrictions and/or one or more usage permissions of the content at a recipient device (D2),
   - generating at the user device (D1) integrity protection information for the at least one defined usage right,
   - encrypting the content with a content encryption key,
   - encrypting the content encryption key with a key encryption key associated with the recipient device (D2) and/or an operator of the recipient device (D2),
   - communicating the encrypted content, the at least one defined usage right, the encrypted content encryption key, and the integrity protection information to the recipient device (D2),
   - verifying at the recipient device (D2) the integrity of the at least one defined usage right based on the integrity protection information,
   - decrypting at the recipient device (D2) the encrypted content encryption key with a decryption key corresponding to the key encryption key,
   - decrypting the encrypted content with the content encryption key in a secure environment (SE2) of the recipient device (D2),
   - applying the at least one defined usage right to the content in the secure environment (SE2), and
   - using the content at the recipient device (D2) according to the applied at least one usage right.

2. The method according to claim 1, wherein the obtained content is content generated at the user device (D1).

3. The method according to claim 1, wherein protected content exists being usage restricted by one or more first usage rights specifying one or more usage restrictions and/or one or more usage permissions of the protected content at the user device (D1), and the content is obtained from the protected content in accordance with the one or more first usage rights by decrypting the protected content by a first content encryption key in a first secure environment (SE1) of the user device (D1) and by accessing the decrypted content in the first secure environment (SE1) for the subsequent steps as far as related to the obtained content.

4. The method according to claim 3 further comprising the step of verifying that the at least one defined usage right is a subset of the one or more first usage rights.

5. The method according to claim 3 or 4 further comprising the step of restricting the one or more first usage rights in consequence of the definition and/or the communication of the at least one defined usage right to the recipient device (D2).

6. The method according to claim 5, wherein the at least one defined usage right comprises a temporal restriction, the method further comprising the step of abolishing the restriction of the one or more first usage rights when the temporal restriction expires.

7. The method according to claim 5, wherein the at least one defined usage right comprises a temporal restriction, the method further comprising the steps of

- blocking or deleting the at least one defined usage right at the recipient device (D2) before the expiry of the temporal restriction,
- communicating an indication of the blocking or deleting to the user device (D1), and
- abolishing the restriction of the one or more first usage rights in consequence of the indication.

8. The method according to claim 7, wherein the indication comprises at least one received usage right being a subset of the at least one defined usage right and the at least one received usage right is applied until the expiry of the temporal restriction and the abolishing of the restriction in consequence of the indication is performed when the temporal restriction expires.

9. The method according to any of the preceding claims, wherein the step of communicating the at least one defined usage right to the recipient device (D2) is executed by
   - communicating the at least one defined usage right from the user device (D1) to a rights server (DS),
   - associating by the rights server (DS) the at least one defined usage right with authorization information indicating a rights issuer authorization for the at least one defined usage right to the recipient device (D2),
   - communicating the at least one defined usage right and the authorization information from the rights server (DS) to the recipient device (D2),

   and the recipient device (D2) verifies the rights issuer authorization based on the received authorization information.

10. The method according to any of the preceding claims further comprising the step of communicating to a charging server an indication about the communication of the at least one defined usage right.

11. The method according to any of the preceding claim, wherein an input unit of the user device (D1) receives at least one instruction from a user for defining the at least one usage right.

12. The method according to any of the preceding claims further comprising the step of defining at least one further usage right for at least one further recipient device for controlling the usage of the content at the at least one further device.

13. A user device (D1) for controlling a usage of content at a recipient device (D2), the user device (D1) comprising at least a transmission unit and a processing unit, wherein the processing unit is adapted to obtain the content, to define at least one usage right specifying one or more usage restrictions and/or one or more usage permissions of the content at the recipient device (D2), to generate integrity protection information for the at least one defined usage right, to encrypt the content with a content encryption key, to encrypt the content encryption key with a key encryption key associated with the recipient device (D2) and/or an operator of the recipient device (D2), and the transmission unit is adapted to send the encrypted content, the at least one defined usage right, the encrypted content encryption key, and the integrity protection information to the recipient device (D2).

14. The user device according to claim 13, wherein the processing unit is adapted to obtain the content from a receiving unit, an input unit, a detector, and/or a storage unit.

15. The user device according to claim 13, wherein protected content exists being usage restricted by one or more first usage rights specifying one or more usage restrictions and/or one or more usage permissions of the protected content at the user device (D1), and the processing unit is adapted to obtain the content from the protected content in accordance with the one or more first usage rights by decrypting the protected content with a first content encryption key in a first secure environment (SE1) of the user device (D1) and by accessing the decrypted content in the first secure environment (SE1) for the subsequent steps as far as related to the obtained content.

16. The user device according to claim 15, wherein the processing unit is adapted to verify that the at least one defined usage right is a subset of the one or more first usage rights.

17. The user device according to claim 15 or 16, wherein the processing unit is adapted to restrict the one or more first usage rights in consequence of the definition and/or the communication of the at least one defined usage right to the recipient device (D2).

18. The user device according to claim 17, wherein the at least one defined usage right comprise a temporal restriction and the processing unit is adapted to check the temporal restriction versus a time signal and to abolish the restriction of the one or more first usage rights if the time signal exceeds the temporal restriction.

19. The user device according to claim 17 further comprising a receiving unit, wherein the at least one defined usage right comprise a temporal restriction and the receiving unit is adapted to receive an indication of a blocking or a deleting of the at least one defined usage rights at the recipient device (D2) and the processing unit is adapted to abolish the

restriction of the one or more first usage rights in consequence of the indication.

20. The user device according to claim 19, wherein the indication comprises at least one received usage right being a subset of the at least one defined usage right and the at least one received usage right is applied until the expiry of the temporal restriction and the abolishing of the restriction in consequence of the indication is performed when the temporal restriction expires.

21. The user device according to any of the claims 13 to 20, wherein the processing unit is adapted to generate an instruction for a rights server (DS) to associate the at least one defined usage right with authorization information indicating a rights issuer authorization for the at least one defined usage right to the recipient device (D2) and to communicate the at least one defined usage right and the authorization information to the recipient device (D2), and the transmission unit is adapted send the instruction and the at least one defined usage right to the rights server (DS).

22. The user device according to any the claims 13 to 21, wherein the transmission unit is adapted to send to a charging server an indication about the communication of the at least one defined usage right to the recipient device (D2).

23. The user device according to any of claims 13 to 22, the user device (D1) further comprising an input unit which is adapted to receive at least one instruction from a user and the processing unit is adapted to define the at least one usage right based on the at least one instruction from the user.

24. The user device according to any of the claims 13 to 23, wherein the processing unit is adapted to define at least one further usage right for at

least one further recipient device for controlling the usage of the content at the at least one further recipient device.

25. A recipient device (D2) for a controlled usage of content, the recipient device (D2) comprising at least a receiving unit and processing unit, wherein the receiving unit is adapted to receive the content being encrypted by a content encryption key, at least one defined usage right specifying one or more usage restrictions and/or usage permissions of the content, a content encryption key being encrypted by a key encryption key associated with the recipient device (D2) and/or an operator of the recipient device (D2), and integrity protection information for the at least one defined usage right, the processing unit is adapted to verify the integrity of the at least one usage right based on the integrity protection information, to decrypt the encrypted content encryption key with a decryption key corresponding to the key encryption key, to decrypt the encrypted content with the content encryption key in a secure environment (SE2), to apply the at least one defined usage right to the content in the secure environment (SE2), and to use the content according to the applied at least one defined usage right.

26. The recipient device according to claim 25, wherein the processing unit is adapted to generate an alert if the integrity of the at least one defined usage right is violated and to initiate an indication of the alert at an output unit.

27. The recipient device according to claim 25 or 26 further comprising a transmission unit, wherein the at least one defined usage right comprises a temporal restriction and the processing unit is adapted to block or delete the at least one defined usage right before the temporal restriction expires and to generate an indication of the blocking or the deleting and the transmission unit is adapted to send the indication to the user device (D1).

28. The recipient device according to claim 27, wherein the processing unit is adapted to generate at least one received usage right that is a subset of the at least one defined usage right for the indication.

29. The recipient device according to any of the claims 25 to 28, wherein the receiving unit is adapted to receive the at least one defined usage right and associated authorization information indicating a rights issuer authorization from a rights server (DS) and the processing unit is adapted to verify the rights issuer authorization based on the received authorization information.

30. A computer program loadable into a processing unit of a user device (D1), the computer program comprising code adapted to execute a process for obtaining of content, to execute a process for defining at least one usage right specifying one or more usage restrictions and/or one or more usage permissions of the content at a recipient device (D2), to execute a process for generating integrity protection information for the at least one defined usage right, to execute a process for encrypting the content with a content encryption key, to execute a process for encrypting the content encryption key with a key encryption key associated with the recipient device (D2) and/or an operator of the recipient device (D2), and to initiate a process for a communication of the encrypted content, the at least one defined usage right, the encrypted content encryption key, and the integrity protection information to the recipient device (D2).

31. The computer program according to claim 30, wherein the code is adapted to execute steps of the method according to any of the claims 1 to 12 as far as related to the user device (D1).

32. A computer program loadable into a processing unit of a recipient device (D2), the computer program comprising code adapted to execute a

process for a verification of the integrity of at least one defined usage right based on integrity protection information for the at least one defined usage right, the at least one defined usage right specifying one or more usage restrictions and/or usage permissions for the usage of content, to execute with a decryption key a process for a decryption of an encrypted content encryption key being encrypted by a key encryption key associated with the recipient device (D2) and/or an operator of the recipient device (D2), the decryption key corresponding to the key encryption key, to execute in a secure environment with the content encryption key a process for a decryption of the encrypted content being encrypted with the content encryption key, to execute a process for applying the at least one defined usage right to the content in the secure environment (SE2) and to control a process for using the content according to the applied at least one defined usage right.

33. The computer program according to claim 32, wherein the code is adapted to execute steps of the method according to any of the claims 1 to 12 as far as related to the recipient device (D2).